U.S. Government Activities to Protect the Information Infrastructure

Dennis D Steinauer, Shirley M. Radack, and Stuart W. Katzke,

U.S. National Institute of Standards and Technology
Gaithersburg, MD USA

Abstract

This paper is a survey of recent activities of the legislative and executive branches of the U.S. Government (and of some joint activities of government and industry) that involve the security of the evolving information infrastructure. Over the past few years, U.S. Government organizations have expanded their use of computer networks to conduct business, deliver services, and share information with industry, other government organizations, and the public. Both government policymakers and program administrators have shown increasing concern about the need for safeguarding the security and privacy of information and about the obstacles that stand in the way of achieving the needed protection. The U.S. Congress has discussed many legislative proposals, including expanded definitions of computer crime, security on the Internet, and export controls on cryptography. The Clinton Administration came into office in 1993 with information technology as one of its principal areas of focus. The Administration also stepped up its information security activities, particularly in support of interagency cooperative efforts for electronic commerce, electronic mail, incident response and information recovery. New avenues for government and industry cooperation were created to solicit industry views and to foster the development of common, interoperable security solutions can be used by both government and industry.. However, the Internet, which has become the *de facto* global infrastructure for information exchange, still lacks strong security-enabling mechanisms. While unique, application-oriented, and non-interoperable solutions are being developed for the Internet, the goal of universal security and interoperability has yet to be achieved.

Introduction

Purpose & Scope

This paper briefly summarizes the activities over the past few years of selected U.S. government organizations that are addressing the challenges of the information infrastructure and provides a listing of electronic addresses for those who would like to obtain more in-depth information.

Background

Information technology continues to undergo rapid and constant change to an extent that cannot be matched by any other technology. For the past two decades, there have been continual, dramatic increases in performance and functionality, accompanied by significantly decreasing prices for information technology products. This rapid change and innovation has impacted almost all businesses and areas of human endeavor, and has enabled the development of new industries, products and services. Information technology systems are widely distributed throughout the world, and tens of millions of people have started to access information through computer networks.

The digitization of information brings a host of new applications and advances the vision of a global information infrastructure, and creates one of the most exciting, promising and challenging periods in the history of technology. Digitization allows voice, text, data, images, video and multimedia to be generated, processed, transmitted, stored and received in a common form or language, and thereby enables multiple functions to come together on common platforms. Increased computational power and bandwidth are leading to new applications combining multiple functions such as electronic commerce, search and

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
24-11-1998	Final Report	xx-xx-1998 to xx-xx-1998

4. TITLE AND SUBTITLE
US Government Activities to Protect Information Infrastructure
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Steinauer, Dennis D ;
Radack, Shirley M ;
Katzke, Stuart W ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
National Institute of Standards and Technology (NIST)
Gaithersburg, MD20899-0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
National Institute of Standards and Technology (NIST)
Gaithersburg, MD20899-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NIST

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES
IATAC Collection

14. ABSTRACT

This paper is a survey of recent activities of the legislative and executive branches of the U.S. Government (and of some joint activities of government and industry) that involve the security of the evolving information infrastructure. Over the past few years, U.S. Government organizations have expanded their use of computer networks to conduct business, deliver services, and share information with industry, other government organizations, and the public. Both government policymakers and program administrators have shown increasing concern about the need for safeguarding the security and privacy of information and about the obstacles that stand in the way of achieving the needed protection. The U.S. Congress has discussed many legislative proposals, including expanded definitions of computer crime, security on the Internet, and export controls on cryptography. The Clinton Administration came into office in 1993 with information technology as one of its principal areas of focus. The Administration also stepped up its information security activities, particularly in support of interagency cooperative efforts for electronic commerce, electronic mail, incident response and information recovery. New avenues for government and industry cooperation were created to solicit industry views and to foster the development of common, interoperable security solutions can be used by both government and industry.. However, the Internet, which has become the de facto global infrastructure for information exchange, still lacks strong security-enabling mechanisms. While unique, application-oriented, and non-interoperable solutions are being developed for the Internet, the goal of universal security and interoperability has yet to be achieved.

15. SUBJECT TERMS
IATAC Collection, NIST, Critical Infrastructure Protection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	22	Usher, Abraham usher_abraham@bah.com
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703289-5678 DSN -

retrieval of multimedia information from digital libraries, and the integration of design, ordering and manufacturing processes.

US Government Roles

The U.S. government has been a leader in adopting the new technology and in working to overcome the technical barriers to its development and use. But at the same time that new applications and systems are being put into place, U.S. policy makers and government officials have become aware of new challenges to the security and privacy of information and to established policies and practices. Many organizations in both the legislative and executive branches have been concerned about security issues including the uses of encryption, export control policies, privacy of information, and network security. These common concerns have stimulated new policies and new practices of cooperation among both government and private sector organizations.

The remainder of this paper will discuss the more significant current IT security issues facing the evolving information infrastructure and the U.S. Government activities to address those issues.

Note on WWW Sources

Much of the material in the section on specific U.S. Government entities and activities was drawn from information on the World Wide Web (WWW). Universal Reference Locators(URLs) for this material is included, where appropriate, in brackets in the text and in a list of URLs at the end of the document.

Areas of Special Interest, Concern, and Challenge

In the last few years, the rapid movement of business and government to highly networked information technology has brought to the front several concerns and challenges. This technology is no longer the province of the scientist and engineer, but has broader societal, legal, commercial, economic, and governmental implications. IT security is central to many, if not most, of these issues. Government, to the extent that its role is to protect the rights of its citizens and provide the basis for an orderly society, has a clear interest This section discusses some of the more significant of those areas of interest, concern, and challenge to the IT security community and the role of government in these areas.

Personal Privacy

Concern over privacy is central to any free society, and people expect the same concepts and controls to apply regardless of technology. However, the nature of information technology (essentially, the "bits" vs. "atoms" comparison of Necroponti[1] and others) has changed -- or at least stretched -- many existing concepts of information privacy. What is clear, however, is that both legal and technological protective measures are needed. Among the areas in which privacy and the confidentiality of information are of particular current concern are the following:

Medical Information

Most people consider medical information -- information about their health status and their relationships with the healthcare community to be of the most intimate and private. However, that very information is the primary currency of the healthcare industry; without it, delivery of quality healthcare would be impossible. The delivery of cost-effective healthcare is dependent, along with other things, on the extensive collection, storage, exchange of such information -- in digital form. It is also quite clear that no amount of concern for personal privacy will slow down this process. Therefore, the availability and effectiveness of IT security measures are critical.

Personal, Business, and Financial Privacy

Along with medical information, there are other types of personal information about which people are increasingly concerned, specifically the detailed information that is maintained as part of their daily

[1] Necroponti, Nicholas., *Being Digital*, Alfred A. Knopf (New York), 1995.

business, financial, and personal lives -- the thousands of transactional records resulting from purchases and other activities -- even their activities on the Internet. Advances in IT have for the first time made the linking and accumulation of individually-identifiable information economically feasible, indeed cheap. Networking technology has made dissemination of and access to such information equally easy and inexpensive. Although there are some controls on "traditional" databases, e.g., credit bureaus (some legislated, others provided out of the economic self-interest of the maintainers), there are now myriad other, uncontrolled ways to obtain private information. Recent examples of commercial offerings of massive personal databases had illustrated the potential and have exacerbated the concern.

Communications Privacy

The impact of information and network technology on communications privacy has been profound, and it has brought into the light of day the basic conflicts between the desire for privacy and the desire of governments to have access to communications for law enforcement and national security purposes. While this used to be primarily a concern for telephonic communication, the melding of all forms of electronic communications (voice, data, video, etc.) into a single form makes the issue one affecting all types of digital information -- stored or in transit.

It has been recognized from the beginning that all public electronic networks, be they voice, data, or whatever, are basically "hostile environments"; there can be no assurance that information is not read or modified in transit. However, except for military and other highly valuable systems, only recently, the designers and users of networks have only recently paid serious attention to security measures to protect those networks from interception or interference. However, the same technologies (primarily cryptography) that provides needed protection can also prevent law enforcement and national security organizations from monitoring communications to which they currently have access.

Monitoring

Along with communications monitoring, advances in information technology also enable increased types of other monitoring of personal activities. Examples include area video surveillance, network activity, use of network services, even satellite (Global Positioning Satellite, direct satellite broadcasting, etc.). All of these types of monitoring require (or should require) security mechanisms and possibly legal protections.

Cryptography Policy

The availability and use of modern, high-speed, digital cryptography is perhaps one of the most controversial and contentious issues in information technology today. As suggested above, this controversy is due to the conflict between the use of cryptography for communications protection (i.e., keeping information unreadable except by the intended recipient) and the need/desire of government to be able to read information for law enforcement or national security purposes. There is a genuine concern on the part of the latter communities that the widespread, unrestricted use of high-quality cryptography (e.g., by criminals) could threaten their ability to protect public safety or national security.

Within the area of cryptographic policy, there are a number of specific areas of current activity and discussion, including the following.

Key Recovery

Key Recovery is the new term, often thought as a substitute for the term *key escrow*. Both refer to the ability to obtain the key(s) necessary to decrypt a specific set of encrypted information. The important distinction is that key escrow is normally used to imply that *government* would hold such keys, while key recovery implies that such keys could be held by other approved parties, with government retaining a right of access under prescribed circumstances. In addition, key recover encompasses the concept of key recovery for emergency purposes by the data owner (e.g., for a lost key or for data encrypted by a terminated employee). The US and other governments have been very actively attempting to resolve the various technical, policy, and legal issues involved. At the same time, the private sector has been moving forward rapidly in an attempt to develop cryptographic solutions that will enable security for electronic commerce and the protection of other information on the net.

Key Management Infrastructure

Irrespective of the issues of key recovery, an important element in the developing commercial network infrastructure will be the deployment of *a key/certificate management infrastructure*. This is needed to enable parties to exchange and cryptographic keys to enable secure communications, even though those parties may not have had prior "introductions". This is also often referred to as the *public key infrastructure*. While several cryptographic products or systems may include a key management process, interoperability across broad domains (companies, industries, and nations) is needed. While most aspects of such an infrastructure may be kept independent of key escrow/recovery issues, there are clear interrelationships that cannot be ignored.

Cryptographic Algorithms

Cryptographic algorithms are of current interest for two reasons. First, current algorithms with relatively short key lengths are becoming vulnerable, and second, governments (the US in particular) place export or import restrictions on certain algorithms, often based on key length.

The reference standard for high quality encryption has been the US Data Encryption Standard (DES), issued by the US National Institute of Standards and Technology (NIST), previously the National Bureau of Standards, in 1977 and revalidated in five year intervals since then. This current standard may be reaching the end of it useful life, efforts are underway by NIST to develop an Advanced Encryption Standard (AES) to eventually replace DES.

There are also several other algorithms in use, but there are restrictions on such use either because they are proprietary and thereby of uncertain strength, or they may be limited from export by the U.S. Government.

Cryptographic APIs

With the possibility of several types of cryptographic algorithms, key lengths, and other factors, it is important that some "common ground" be found to enable interoperability among different users, applications, and networks, and to remove the necessity for system developers to become cryptographic experts. The development of common cryptographic application interfaces (CAPIs) has, therefore, been a significant area of interest in the last few years.

The Internet

The seemingly explosive growth of the Internet beyond the scientific, educational, and government domains has in itself become a major security concern (and driver) for the entire IT community. Not only has it changed the extent to which information is available and the ability of people to communicate, it has challenged traditional models of technology management and security. Indeed, virtually all the other areas of concern discussed in this entire section were probably brought to the public's attention more by the Internet than any other reason. Among the more significant areas of concern with the Internet are the following.

Management & Control

The very nature of network technology in general and the Internet in specific defy traditional concepts of management and control. The Internet and its communications protocols were designed to be resistant to single points of failure and to be able to survive even massive segment outages. In essence, it is *designed* to operate without central control. Therefore, attempts to "protect" activities on the Internet through traditional management and control techniques are meeting considerable difficulty. Many, including governments and corporations, are finding hard to accept the idea that "no one is in charge" of the Internet.

Security & Privacy

Although the eventual need for security was understood by the early developers of the Internet, it was clearly a barrier to the free and open communication that such networks enabled -- to the point that security mechanisms were often viewed as the antithesis of the "Internet ethic". As use grew, however, it

was recognized that protecting the integrity and privacy of one's information was just as valid on the net as it is in other areas of society. The need for effective, interoperable security mechanisms has been further highlighted by increasing commercial use of the Internet and business' recognition that security is, indeed, one of their utmost requirements.

Increasing Dependence

As with many technologies, once people began using the Internet, they wondered how they ever go along without it and became increasingly dependent on its availability and reliability. In the last year or so there have been several examples of how malicious activity can effectively deny access to the net or to needed resources to other users. The *availability* aspect of information security has now become equal to *confidentiality* and *integrity* in the concerns of users, managers, and even governments (see below).

Impact on society, commerce, national security

As mentioned earlier, the nature of information technology has challenged traditional concepts and models for commerce, "property", government, and society in general. The Internet, because it has expanded so broadly, deeply, and rapidly, has forced us to face those challenges earlier than we might have planned.

Information Warfare

The national security establishment has long been a major (indeed, probably the largest) user of information technology and has always recognized the need for security. Indeed, a great deal of the early and most technically advanced work in the area was conducted by or for the national security and intelligence communities. Even this community, however, has only recently recognized on the strategic offensive and defensive aspects of IT -- an area now called *information warfare*. While the private sector and the civilian side of government are generally not involved with *offensive* information warfare, they are increasingly concerned with *defensive* information warfare, since this involves protective measures that often have applicability even in less that "war time" situations.

Critical Technologies Control

The U.S. Government has always exercised controls and other protective measures to ensure that materials and technologies deemed critical to the "national security" (however defined at a given time) are available to the US when needed and, if possible, denied to our potential adversaries. These same concerns exist with information technology, with the added complication that such technologies (often being "bits rather than atoms") are often much more difficult to control.

Law Enforcement

It is one of the responsibilities of governments to enforce their laws, thereby providing a degree of protection to the rights, person, and property of their citizens. Information technology presents challenges and opportunities to government in this area. Law enforcement has only in the last few years begun to develop the basis for understanding the legal implications of IT and how IT can be both a tool and a target of criminal activity, and acquiring the skills and knowledge to use the technology in its own work.

Applicability Of Existing Laws In "Cyberspace"

Although it is accepted generally that legal concepts, principles (e.g., property, ownership, contracts, fraud, etc.) apply regardless of the environment, it is now clear that the IT domain (now often called "cyberspace") has some unique characteristics that make applicability of these concepts and principles difficult (at best). The elements of time, place, and physical entities are often lost or changed in their meaning.

Criminal Activity In "Cyberspace"

A second area of concern to law enforcement and citizens alike is the new opportunity that information technology provides for criminal activity -- both as a tool and as a target for such activity.

International Economic Issues

Although most of the issues discussed above have clear international aspects, the Internet has brought a truly global perspective on economics and commerce. A number of key issues must be faced as information technology becomes the international medium of business and government.

Intellectual Property Protection

Intellectual property -- those non-physical things such as ideas, algorithms, music, software, etc. that often exist in physical form on some type of digital medium -- has become perhaps the most valuable of all types of property. With the movement to representation, storage, and transmission of intellectual property in digital instead of physical form (i.e., "bits" vs. "atoms"), new protection mechanisms become of critical importance. As a result, the need for protection of *all* forms of intellectual property (not just "traditional" data) has driven the demand for effective IT security mechanisms.

Telecommunications Reform

Until very recently, telecommunications was a monopolistic, mostly government-controlled enterprise. This not only gave national governments the ability to provide universal service, it also gave them a high degree of control over international interactions. In virtually all democratic nations, almost all telecommunications (broadcast and direct) have become more decentralized, private-sector, competitive activities. The merging traditional forms of telecommunications (voice, video, etc.) into a single digital stream has resulted in a vast, single, integrated form of communications which both demands and defies traditional methods of management and control. Data security needs now apply to all forms of communications, and the lack of single "points of control" requires extraordinary cooperation among industry and government.

Regulation

As suggested in the previous paragraph, the issue of regulation (government or otherwise) is central to current activities in both telecommunications in general and security in particular. Many have expressed frustration at the fact that "no one is in charge" of the Internet, and thus traditional legal and regulatory methods of addressing many issues do not work. Nevertheless, there is a great deal of control that governments still have over both the underlying telecommunications carrier technology, both terrestrial and space-based. Therefore, despite many inherent "boundary" problems with the actual activities in "cyberspace", there are some controls that governments can exercise.

Electronic Commerce

Although implicit in most of the foregoing discussion, the concept of electronic commerce, i.e., conducting business electronically, over telecommunications networks, is perhaps the most important unifying theme of the last ten or so years and into the future. In the same way that a wide array of traditional business controls (e.g., double-entry accounting, signed contracts, audit trails, etc.) have protected traditional commerce, corresponding security mechanisms are required for electronic commerce. The key difference, as with several of the other areas discussed above, is the fact that physical entities, records, and control mechanisms (i.e., the atoms) are less applicable, since most of these are replaced with their digital forms (the "bits").

Although the movement to electronic commerce (and the need for security) has been underway for several years, only with the explosion of Internet activity has there been true recognition that existing security mechanism (at least those that have been actually implemented on a wide-scale basis.

Pornography and Free Speech

The international aspect of the Internet has brought to the forefront difficult issues that are colored by culture, national, political, religious, ethnic, and every other sort of societal differences. To the extent that the net has few, if any, boundaries, the many (perhaps most) activities on the net are sure to conflict with customs, rules, beliefs, or preferences based on those differences. Recent incidents of government actions to restrict certain activities on the net, legal proceedings against users or groups of users, and similar activities point to the difficulties at hand. Many consider activities on the net primarily and issue of free speech, but not all nations and cultures have a common concept of even this. Fortunately (at least for the technologist), most of these issues are political and legal, not technical. However, it will be the IT security community that will be called upon the help develop and implement the mechanisms demanded by society..

Critical Infrastructure Protection

Finally, as nations reexamine their vital national interests, they have begun to recognize that even the traditional "physical" infrastructures upon which their economies (and to a large extent, their national security) are based are themselves increasingly controlled by information technology. Thus, vulnerabilities in that technology or the systems built with IT can result in vulnerabilities or fragility in the infrastructure(s) it helps control. The U.S. Government has recently become much more involved in this area.

Conclusions

This section has discussed just some of the many significant issues that must be addressed as we move to a more network-based society. The following section describes many of the elements of the U.S. Government and related entities that have a role in addressing these issues and some of the significant recent activities in the area of IT security.

Significant US Government IT Security Roles, Responsibilities, and Activities

US Congress

Over the past several years, the US Congress has shown increasing interest and growing understanding of the nature and importance of information technology and the potential national policy issues related to that technology. Some of these issues are the following:

Cryptography And Export Controls

Concerned about restrictions on the export of encryption capabilities, controls, the Congress considered legislation that would: ensure that Americans could choose any security system to protect their confidential information and not be restricted to encryption devices with limited key sizes; prohibit the requirement for a key escrow system to enable encryption keys to be made available for law enforcement and national security purposes; make it unlawful to use encryption in the commission of a crime or to willfully cover up a crime; and allow the U.S. computer industry to export generally available software and hardware if a product with comparable security is commercially available from foreign suppliers. The legislators pursuing this issue were concerned that many foreign products and programs with strong encryption capabilities were available in the world marketplace, and that of U.S. companies were disadvantaged with restraints on the export of strong encryption products.

Critical Infrastructure Hearings

There was Congressional concern about the potential vulnerabilities of the information infrastructure, and the need to provide for security not only for computers but for other vital systems as well. It was recognized that many critical elements of the infrastructure --power, communications, financial,

transportation--are largely in the hands of the private sector. As these critical elements become more reliant upon open computer networks, there will be greater need for government to partner with industry to ensure the reliability of the systems they support. The need for reliable threat estimates by intelligence and law enforcement agencies was cited as a way to secure government and military systems, and to provide data to the private sector so that they can manage their own risks. Also noted as pivotal to addressing this issue was the need for trust between industry and government, and for international alliances to address problems transcend national boundaries.

Crime Legislation And Hearings

The Congress considered legislation to address the problem of computer-age blackmail. This was characterized as a high-technology variation on extortion, such as a person threatening to crash a computer systems unless he was given free access to the system and an account. The crime legislation would strengthen law enforcement's ability to prosecute persons who threaten to harm or shut down computer networks unless their extortion demands are met, or who abuse computers, or steal classified or valuable information or commit other crimes.

Telecommunications legislation

Telecommunications legislation was introduced to eliminate barriers to market entry, increase competition, and to help to advance diversity of ownership in the telecommunications marketplace. This legislation followed a major overhaul of the Telecommunications regulations enacted by the previous Congress.

Other security-related legislation and hearings

Public Law 104-13, Paperwork Reduction Act of 1995, was enacted. This legislation addressed the ongoing Congressional interest in minimizing the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information by or for the Federal Government and to improve the public benefit from information created and collected by the Federal government. Among its provisions were requirements for uniform Federal information resources management policies and practices, including appropriate measures to protect the privacy and security of information.

Public Law 104-106, Information Technology Management Reform Act of 1996, focused on improving the acquisition, use, and disposal of information technology by the Federal Government. The legislation changed acquisition authorities and requirements. Agencies were given authority to manage their information technology acquisitions. Agencies were required to establish Chief Information Officers, reporting directly to the heads of the agencies, and providing information technology advice and assistance. Further the legislation re-enacted the Computer Security Act of 1987, which established NISTs programs to develop standards and guidelines to protect the Federal government’s unclassified information that is processed by computers.

Significant Legislation

Although the U.S. Congress passed many bills that had impact on information technology in general and some IT security implications, there are a few bills that have particular impact on the security community and the evolving information infrastructure.

Telecommunications Act of 1996

Public Law 104-104, Telecommunications Act of 1996 was major legislation enacted in 1996 which changed the telecommunications marketplace by promoting competition in many sectors.. The goal was to reduce the high costs to telecommunications companies of compliance with regulations, to shorten the length of licensing procedures, and to reduce, the uncertainty of the outcome of licensing procedures. It was felt that more competition would stimulate new market conditions and innovation..

Communications Decency Act

Enacted as Title V (Obscenity and Violence) of the Telecommunications Act of 1996, this legislation revised existing legislation to prohibit obscene or harassing telephone calls and conversation in the use of a telecommunications facility and communication. It prohibited communication which is obscene, lewd, lascivious, filthy, or indecent with intent to annoy, abuse, threaten, or harass another person and prohibited making obscene communication available to minors. One provision directed the Federal Communications Commission to determine whether video programming distributors voluntarily established rules for rating programming that contains sexual, violent, or other indecent material. Rating systems would enable parents to monitor what their children can view and to block inappropriate programming. The FCC was directed, to require apparatus designed to enable viewers to block display of all programs with a common rating.

National Information Infrastructure Protection Act of 1996

National Information Infrastructure Protection Act of 1996 was introduced into the Senate, but not enacted. The legislation was intended to help safeguard the privacy, security, and reliability of national computer systems and networks and the information stored in, and carried on, those networks. Since such systems were perceived to be vulnerable to the threat of attack by hackers, high-technology criminals and spies, the Act updated the criminal code to ease the difficulties that law enforcement officials experienced in fighting crimes targeted at computers, networks, and computerized information.

Other Security-Related Bills

The Electronic Freedom of Information Improvement Act of 1996, Public Law 104-272 extended the Freedom of Information Act which requires agencies of the Federal Government to make certain agency information available for public inspection and copying. Since Government agencies are increasingly using computers to conduct agency business and to store publicly valuable agency records and information, the Act requires agencies to use their new technology to enhance public access to agency records and information. By facilitating the dissemination of Federal information, the Act attempts to maximize the usefulness of agency records and information for the public.

Executive Office of the President

The Executive Office of the President (EOP) provides overall management policymaking and direction for the entire Executive Branch of the U.S. Government. This is accomplished through several mechanisms, including Executive Orders, various committees reporting directly to the president or vice-president, and the Office of Management and Budget.

Executive Orders

Many policy decisions and initiatives within the U.S. Government are effected through the issuance of presidential Executive Orders. Several recent Executive Orders relate directly to information security issues.

Executive Order 13026, Administration of Export Controls on Encryption Products

This executive order transfers certain encryption products from the United States Munitions List administered by the Department of State to the Commerce Control List administered by the Department of Commerce. The E.O. provides for controls on the export and foreign dissemination of encryption products transferred to the Department of Commerce. The export of encryption products transferred to Department of Commerce control could harm national security and foreign policy interests of the United States even where comparable products are or appear to be available from foreign sources. The E.O. allowed the Secretary of Commerce to consider the foreign availability of comparable encryption products in determining whether or issue a license or to remove controls on particular products. However, the Secretary is not required to issue licenses in particular cases or to remove controls on particular products based on foreign availability. The E.O. stated that appropriate controls on the export and foreign dissemination of encryption products may include measures that promote the use of strong encryption products and the development of a key recovery management infrastructure.

Executive Order 13010, Critical Infrastructure Protection

established the President's Commission on Critical Infrastructure Protection, to identify and consult with the public and private sectors, assess the scope and nature of the vulnerabilities of the critical infrastructures, review legal and policy issues, and recommend a national policy and implementation strategy for protecting critical infrastructures from physical and "cyber" threats. The members of the commission include representatives from certain U.S. government agencies and their nominees who could be individuals from the private sector.

Executive Order 13011, Federal Information Technology

This order establishes the policies to enable Federal agencies to carry out the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996. Policies relate to agency acquisitions and to interagency support activities. Federal government responsibilities to develop and use information security standards are reinforced.

National Security Council

The National Security Council is the President's principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials. The Council advises and assists the President on national security and foreign policies, and coordinates policies among agencies. Members include the President, the Vice President, and the Secretaries of State and Defense. Others contributing to the NSC include the Chairman of the Joint Chiefs of Staff, the Director of Central Intelligence, the Secretary of the Treasury, the U.S. Representative to the United Nations, the Assistant to the President for National Security Affairs, and the Assistant to the President for Economic Policy. The NSC is involved in science and technology issues related to U.S. economic competitiveness and national security.

National Economic Council

The National Economic Council coordinates the economic policy-making process with respect to domestic and international economic issues; coordinates economic policy advice to the President; ensures that economic policy decisions and programs are consistent with the President's stated goals, and that goals are being effectively pursued and implemented.

Special Committees, Task Forces, and Other Groups

In addition to specific agency activities, there are a number of special committees, task forces, and other groups, comprising representatives from several agencies, that address issues relating directly or indirectly to IT security. These are, essentially, government-only groups and are distinguished from special government-industry commissions and advisory boards. (See Advisory Boards and Other Avenues for Solicitation of Industry Views)

Federal Networking Council

The Federal Networking Council (FNC) is chartered by the National Science and Technology Council's Committee on Computing, Information and Communications (CCIC) to act as a forum for networking collaborations among Federal agencies to meet their research, education, and operational mission goals and to bridge the gap between the advanced networking technologies being developed by research FNC agencies and the ultimate acquisition of mature version of these technologies from the commercial sector National Information Infrastructure and Information (DDS) Infrastructure Task Force
[http://www.fnc.gov/]
Privacy & Security Working Group (PSWG) The Privacy & Security Working Group is responsible for addressing network security technology, management, and administration issues related to maintaining and improving the availability, integrity, and confidentiality of Interagency Internet resources. It will also review security requirements of the evolving NREN and propose technical developments, operational guidelines, and administrative procedures needed to meet them. It prepares input to the FNC, as needed, on security related matters. The PSWG works closely with other organizations developing or defining security policies, standards, services, and mechanisms in fulfilling these duties.
]http://www.fnc.gov/FNC_wg.html]

Office of Management and Budget

The Office of Management and Budget assists the President in overseeing the preparation of the Federal budget and supervising its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's budget and with Administration policies. In addition, OMB oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies. In each of these areas, OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public. Under the Computer Security Act, OMB is responsible for planning and policies to protect the security and privacy of information in Federal computer systems. OMB Circular A130, Appendix III, establishes a minimum set of controls to be included in Federal automated information security programs; assigned Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems.

Commerce Department

National Institute of Standards and Technology (NIST)

The mission of the National Institute of Standards and Technology (NIST), specifically its Information Technology Laboratory (ITL) and the Computer Security Division (CSD) is to work with industry and government to develop technology and testing processes to improve and ensure the security of information technology systems and networks. Within the U.S. Government, NIST has the lead role for the security of information technology systems (except for classified and national security related systems, which are the domain of the National Security Agency, NSA). It should be noted that NIST's responsibility is to provide federal agencies with standards and guidance to improve the protection of agency IT systems; it is the responsibility of each agency (i.e., not NIST) to apply appropriate security measures and ensure protection of each IT system, network, resources, and information.
NIST undertakes a number of programs that are designed to fulfill these roles.

Conformance Test Center Initiative

A cross-cutting activity for the Information Technology Laboratory is the development of a comprehensive, industry-driven, conformance testing function. This function will support the testing

needs of the different technologies addressed by each ITL division. The common objective is to ensure the development of tests and test methods necessary for this increasingly complex and difficult area of technology. Within the Computer Security Division, these activities will impinge on each of the major projects described below.

The ITL Test Center is partitioned into two functional areas: a testing research function and an applied function. The research function is focused on developing the test methods, tests, and tools; the applied testing function is focused on applying technology transfer by assisting organizations to develop strong conformance testing programs. Tasks supporting the ITL Test Center are part of several different projects, both in the Computer Security Division (and in other parts of ITL)

The Computer Security Division

The Computer Security Division (CSD) within ITL is responsible for NIST's Computer Security Program. The CSD works with industry and government to establish secure information technology systems by developing methods for protecting the integrity, confidentiality, reliability, and availability of information resources; enables the measurement and improvement of the security of information technology systems and networks; addresses such technical areas as: cryptographic based techniques, advanced authentication systems, communications security, public key certificate management, firewall policy and design, incident response, vulnerability analysis, security architectures, and security criteria and metrics; and produces standards, guidelines, prototypes, conformance tests, validated products, assurance metrics, and reference implementations.

The CSD major projects are described below.

Cryptographic Technology and Applications

The goal of the Cryptographic Standards, Guidance, and Applications project is to develop standards and guidance on the use of cryptographic technology and to provide for conformance testing of vendor products so that strong cryptographic mechanisms will be available for the protection of sensitive information. Even today, most users do not have the technical skills and knowledge to evaluate cryptographic products and systems for quality and effectiveness. Cryptographic standards may provide interoperability and an acceptable level of security. Testing of products which were built to conform to the standards verifies that the provisions of the standard were correctly implemented. Many weaknesses occur upon implementation. Until recently, NIST only performed simple testing of cryptographic algorithms. This project has now begun the more complex testing of cryptographic modules and is planning to test entire systems in the future.

Advanced Authentication Technology

The primary goal of the NIST Advanced Authentication Technology Program is to further the development and widespread use of secure and cost effective authentication technologies. NIST has worked closely with private industry and other government agencies for the last several years to identify and address the technical challenges which must be overcome to meet this goal. The first challenge is to develop a framework that identifies the functional components and interfaces required to support a common authentication architecture capable of spanning heterogeneous authentication domains. Some of these components and interfaces exist today; some will need to be built. Second, standardized interfaces between host systems and authentication modules will be required as a common target for applications developers, operating system vendors, and authentication technology providers. Third, a common interdomain language for transfer of authentication data is needed, independent of the protocols used within a domain for authentication. Finally, NIST should continue to promote and participate in the development of strong authentication protocols based on cryptographic techniques. Major task areas within the Advanced Authentication Technology Program correspond to the technical challenges described above.

Public Key Infrastructure

Public Key Infrastructure (PKI) is a collection of systems that exist with the purpose of generating, revoking, disseminating, and otherwise managing public key certificates. Public key certificates are data

entities that bind the identity of communicating parties to their public keys. The use of public key cryptography is central to the widespread use of digital signatures. This technology can be used to enable user authentication, message integrity, and message non-repudiation services essential for the general acceptance of electronic commerce and other electronic services. The purpose of this program is work with both government and industry to develop public key based security for distributed applications among Federal government agencies, industry, and diverse communities such as the Internet. The primary objectives are to:

- In conjunction with the Federal government and industry, develop PKI specifications which promote the development of Commercial Off-The-Shelf products that meet the security requirements of government and commercial applications.
- Develop guidance on the implementation and use of PKI technology.
- Implement PKI technology developed by NIST and its business partners and integrate this technology into electronic based information applications.

Internetworking Security

The Internetworking Security Project's primary goal is to provide computer security assistance to current and future users of the Internet. The Internet is undergoing dramatic growth, with businesses and government at all levels connecting to the expanding it. Business and government are in the initial stages of conducting electronic commerce on the Internet, using it for purchasing and business communication needs. Yet, the security infrastructure of the Internet is very weak, such that serious security vulnerabilities and threats such as intruders can cost users millions of dollars in lost time and productivity. Easy solutions do not exist, and many users throughout government and industry are searching for guidance and common solutions. The purpose of the Internet Security program is to:

- provide immediate assistance to government and industry users in securing their systems and sites;
- educate organizations in areas such as Internet security policy, firewalls, and security tools;
- provide coordination to incident response activities;
- examine and influence long-term security solutions and potential problems with emerging networking technologies, and
- work with industry to facilitate information exchange, develop common solutions to infrastructure problems, and improve the ability to conduct electronic commerce.

NIST plans increasingly to shift Internet security project work towards emerging high-speed technologies and towards industry needs in the areas of electronic commerce, telecommuting, and virtual research enterprises.

Criteria and Assurance

The Criteria and Assurance project provides improved metrics and methods required to specify, build and evaluate advanced information technology (IT) security products and systems. Tasks under the Criteria and Assurance project focus on improving the infrastructure to support widespread commercial availability of security technology.

The Criteria and Assurance Project has four main objectives:

- lower the cost of producing security-capable IT products,
- increase the commercial availability of security-capable IT products,
- broaden the global market for US made security-capable IT products; and
- allow market forces to determine the characteristics of security-capable IT products

A growing market exists for security-capable products that are effective, useful, reliable and affordable. Traditionally, the characteristics of security-capable products are determined by governmental evaluations

against a predefined criteria. Several countries evaluate security-capable IT products including the US, Canada, France, Britain, Netherlands, and Germany. Current evaluation criteria, schemes and methods produce products that are expensive and of limited utility. The alternative is ad-hoc methods and untried products that provide questionable protection and can be dangerous if used to protect highly valuable computerized assets. The Security Criteria and Assurance Project is designed to address the shortcomings of current evaluation criteria, schemes and methods while preserving the advantages gained from using products of known security characteristics.

Security Management and Support

In addition to the work in each of the projects above, the NIST computer security program undertakes several activities to enhance the ability of organizations to manage effectively their security programs. This includes a wide range of activities such as providing technical and management guidance to government agencies, support for the Computer System Security and Privacy Advisory Board (CSSPAB) and the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure (see below), the National Information Systems Security Conference, and other forms of user awareness and education support. Of particular note is the NIST Computer Security Resource Clearinghouse (CSRC), a world wide web containing a wide range of information and links to other information source.
http://csrc.nist.gov

Key Escrow System

The Key Escrow System is a project in support of the Escrowed Encryption Standard (FIPS-185) and Presidential Decision Directive/NSC-5. The primary objective of this program is to provide the U.S. Government and the private sector with high-quality, secure communications products without jeopardizing effective law enforcement, public safety, and national security. The initiative is based on a special tamper-resistant hardware encryption device (Clipper/Capstone Chip) and a Key Escrow System (KES). The KES program is interagency, with support from the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Department of Treasury, and the National Security Agency (NSA). The central principle of the Key Escrow System system is that no single agency or individual holds sufficient information or capabilities to violate the security of the Key Escrow system or the security of the product in which the escrowed encryption devices are installed. In particular, each device is controlled by a different agency of the government and the cooperation of all Agents is required to operate the system.

Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure

Use of strong cryptography on a widespread basis in the Global Information Infrastructure requires a supporting infrastructure, including the provision of many services (e.g., authentication, trusted notary, etc.) One important service is key recovery (for keys used for confidentiality). This will help protest users when keys are lost or destroyed, and also assist law enforcement decrypt information under lawful circumstances. To facilitate provision of key recovery services for its own use, the government needs a Federal Information Processing Standard. The standard must be developed by working with those who produce and use cryptographic technologies in the private sector. The Advisory Committee, comprised of private sector individuals, will be an important vehicle by which the government gains the benefit of private sector input in developing this standard. To a certain extent, the committee resembles the standards development committees utilized by the private sector; however, it is intended that this Committee provide technical recommendations to the Secretary of Commerce on the development of a standard.
When completed, the standard will enable key recovery services for use within the government which are compatible with private sector activities. The Advisory Committee's work will gain from the experiences of the key management infrastructure pilot projects, including key recovery services, underway within the government, which can provide useful input and real-world experiences for the committee. The Committee's work will take place concurrently with (and not supplant) many ongoing private and public sector activities, such as those in the area of public key infrastructure. When adopted, the standard will be

available to the public and private sector (on a voluntary basis) for providing key recovery services. The Committee's assignment, as discussed in the charter, is to make technical recommendations regarding the development of a draft FIPS for Cryptographic Escrow Systems which could be incorporated into a Federal Key Management Infrastructure. The Committee will focus on the data recovery services of the Federal Key Management Infrastructure for both stored and communicated information.

Federal Computer Incident Response Capability (FedCIRC)

The Federal Computer Incident Response Capability (FedCIRC) is a new initiative undertaken by the National Institute of Standards and Technology (NIST), the Department of Energy's Computer Incident Advisory Capability (CIAC), and the Carnagie Mellon, Software Engineering Institute's CERT/CC. These established computer security organizations have banded together to offer the Federal civilian community assistance and guidance in handling computer security related incidents.

On June 3, 1996, the Government Information Technology Services (GITS) Innovation Fund Committee granted $2,796,000 to the National Institute of Standards and Technology to establish a Federal Computer Incident Response Capability (FedCIRC). The capability, which is now operational, assists federal civilian agencies in their incident handling efforts by providing proactive and reactive computer security related services.

NIST subcontracts the operational incident handling capability to the Defense Advanced Research Project Agency's CERT(sm) Coordination Center (CERT/CC) and to the Department of Energy's Computer Incident Advisory Capability (CIAC). NIST is responsible for operational management and for facilitating the development of incident handling standards and guidelines by utilizing the vulnerability data collected by FedCIRC. The vulnerability information will also be used in the analysis and testing of software and other products.

FedCIRC combines the experience and expertise of NIST's Computer Security Division, CERT/CC, and CIAC to provide agencies with cost reimbursable, direct technical assistance and incident handling support.

Bureau of Export Administration (BXA)

The Bureau of Export Administration is concerned with U.S. security and economic prosperity as they relate to the control of exports for national security, foreign policy, and short supply reasons. The Bureau administers the Export Administration Act; develops export control policies; issues export licenses; and enforces antiboycott provisions.

In August 1995, the U.S. decided to ease export licensing requirements for key escrow encryption software products. As part of this decision to allow the export of these products, BXA developed draft criteria for key escrow products and for key holders. Products that conform to these criteria will be considered for transfer from the U.S. Munitions List to the Commerce Control List following a case-by-case determination by the Department of State through the commodity jurisdiction procedures. BXA prepared in 1996 regulations to implement the Administration’s encryption policies based upon a 1996 announcement of plans to make it easier for Americans to use stronger encryption products to protect their privacy, intellectual property and other valuable information.

U.S. Patent and Trademark Office (PTO)

The Patent and Trademark Office promotes industrial and technological progress in the United States and strengthens the national economy by administering the laws relating to patents and trademarks; advising the Secretary of Commerce, the President of the United States, and the administration on patent, trademark and copyright protection and trade-related aspects of intellectual property. PTO examines and issues patents to encourage technological and advancement by providing incentives to invent, invest in, and disclose new technology worldwide. Through the registration of trademarks, PTO assists businesses in protecting their investments, promoting goods and services and safeguarding consumers against confusion and deception in the marketplace. By disseminating both patent and trademark information, PTO

promotes an understanding of intellectual property protection and facilitates the developments and sharing of new technologies world wide.

Department of Defense

National Security Agency (NSA)

The National Security Agency/Central Security Service (NSA/CSS) is responsible for the centralized coordination, direction, and performance of highly specialized technical functions in support of U.S. Government activities to protect U.S. communications and produce foreign intelligence information. The Central Security Service (CSS) was established a unified cryptologic organization within the Department of Defense. NSA/CSS are organized to accomplish two national missions. The first mission is information systems security or INFOSEC mission which provides leadership, products, and services to protect classified and unclassified national security systems against exploitation through interception, unauthorized access, or related technical intelligence threats. This mission also supports the Director, NSA, in fulfilling his responsibilities as Executive Agent for interagency operations security training. The second mission, foreign signals intelligence or SIGINT mission, allows for unified organization and control of all the foreign signals collection and processing activities of the United States.
Within the NSA, the National Computer Security Center promotes the availability of trusted systems, commercially produced and support systems with technical protection capabilities.

Defense Advanced Research Projects Agency (DARPA)

DARPA's primary responsibility is to help maintain U.S. technological superiority and guard against unforeseen technological advances by potential adversaries. DARPA develops imaginative, innovative and often high risk research ideas offering a significant technological impact that will go well beyond the normal evolutionary developmental approaches; and pursues these ideas from the demonstration of technical feasibility through the development of prototype systems.

Defense Information Systems Agency (DISA)

DISA is the Department of Defense (DOD) agency responsible for information technology and is the central manager of major portions of the Defense Information Infrastructure (DII). DISA is responsible for planning, developing, and supporting Command, Control Communications, Computers, and Intelligence (C4I) that serve the National Command Authority (NCA) under all conditions of peace and war. Within the DISA, Agency, the Joint Interoperability and Engineering Organization's Center for Standards is responsible for executing the duties of the Executive Agent for DOD Information Technology (IT) Standards, including the development, adoption, specification, certification, and enforcement of information processing, transfer and content standards within DoD. This includes influencing the development and adoption by industry of standards supporting DoD requirements.

Department of Treasury

Through its information technology management activities, the Department of Treasury has been active in improving U.S. Government functions through better use of information technology. The goal is to make government services more accessible, more efficient, and easier to use, and to promote the development and implementation of information technology infrastructure to make "electronic government" a reality.

International Activities

Information technology is a global concern. Not only is the technology itself common and ubiquitous, but data networks (e.g., the Internet) are inherently transborder, multi-national (some would argue, extra national) entities. International cooperation (and, to some extent, coordination) is critical. The U.S. Government is a primary participant in a wide range of international activities affecting IT security. Some of these are purely government/diplomatic activities, while others are basically private sector

activities in which representative(s) of the U.S. Government participate. The following are some of those activities.

Organisation for Economic Cooperation and Development (OECD)

The OECD's work on economic and policy issues in the fields of information and communications technologies and infrastructures is conducted under the aegis of the Information, Computer and Communications Policy (ICCP) Committee. In addition to specific studies of information technology(IT), telecommunications, and related legal and standardisation questions, ICCP also tackles issues of technology and policy convergence, diffusion and impact on the economy and society. Although it had used the term in published work as early as 1977, ICCP has made "information infrastructure" itsexplicit medium-term focus since 1993. The Secretariat has reviewed the information infrastructurepolicies proposed by national governments and international bodies. In May 1996, the Counciladopted a number of policy recommendations for "global information infrastructure - global informationsociety", and the ICCP is currently preparing a substantial background report.

- Telecommunications
- Economics of the Information Society
- High Performance Computing and Networking
- Security, privacy, cryptography and intellectual property rights
- IT standards
- ICCP Publications
- OECD Tokyo Multimedia Symposium
- Policy documents freely available for downloading
- Current Status of Communication Infrastructure Regulation: Cable Television

[http://www.oecd.org/dsti/sti_ict.html]

Work in the OECD on protection of personal data and privacy, security of information systems, cryptography policy, and protection of intellectual property is directed toward worldwide harmonization. This goal is reflected in the international instruments of the OECD in these fields. Many advanced technologies, such as information and communications technologies, directly raise questions aboutthe nature, role and scope of sovereignty and government. Information and communicationstechnologies and their projected rates of development and use, as well as the convergence of thesetechnologies with other scientific and technological disciplines, such as biology, biotechnology andnanotechnology, create conditions that require a reconsideration of existing national rules and theestablishment of global consensus on new rules. It is widely recognised, with regard to matters linkedto powerful, dynamic and pervasive information and communication technologies, that individualnational solutions, are, for the most part, inefficient and potentially anti-competitive for that nation'seconomy.

The OECD Member countries as well as non-Member countries adopt legislation based on the OECD Privacy Guidelines and Security Guidelines. In addition to legislation, they also establish standards, technical criteria, and other regulations. Hundreds of private sector entities have adopted theGuidelines and use them as a basis for codes of conduct and internal management, administrativeand technical procedures. It is to be anticipated that additional OECD work in these areas will betaken up in the same practical manner.

[http://www.oecd.org/dsti/iccp/legal/top-page.html]

Security Guidelines

In 1988, the OECD Member countries asked the OECD Secretariat to prepare a comprehensiveanalytical report on security of information systems, covering technological, management,administrative, and legal matters. Following from this work and recognising that explosive growth inthe use of information systems, for all types of applications in all parts of life, had made provision ofproper security essential, the

OECD Member countries negotiated and adopted the 1992 OECDGuidelines for the Security of Information Systems. The Guidelines provide an international frameworkfor the development and implementation of coherent security measures, practices and procedures inthe public and private sectors. The Recommendation of the Council of the OECD Concerning Guidelines for the Security ofInformation Systems recommends that OECD Member countries review the Guidelines every fiveyears with a view to improving international co-operation on issues relating to the security ofinformation systems. The Guidelines were adopted in 1992. In accordance with the Recommendationof the Council, OECD Member countries will review the Guidelines in 1997.
[http://www.oecd.org/dsti/iccp/legal/secur-en.html]

Cryptography

In 1992, the OECD began to hold meetings on the subject of cryptography technologies and policies. Interest in these subjects has continued to increase. Cryptographic methods have been employed for thousands of years. In the modern era, mathematics and computing science have been increasingly used in cryptography. Formerly the domain of military and national security agencies, the conception of cryptography and its applications is in transition. From munitions for use by the few, encryption is coming to be considered as part of the toolkit of all computer users. A good analogy is the password. Twenty years ago, only spies and soldiers used passwords. Today, even school children have them. It is now widely recognised that there are legitimate commercial, administrative, and individual needs and uses for cryptography. It will be important to the provision of security, privacy and intellectual property protection in the GII and the growth of many applications such as electronic commerce, credentials and voting. Businesses, civil ministries and citizens wish to use cryptography to protect the product designs, tax and health records, and love letters that will be transmitted on the information infrastructure. The challenges ahead are to increase public awareness of cryptography and its potential uses and to build consensus on an international cryptography policy and the respective roles of government, industry and the individual. The OECD created an Ad hoc Group of Experts to draft Cryptography Policy Guidelines which will provide internationally comparable criteria for cryptography policy-making. The Group met for the first time in Washington DC in May, a second time in Paris in June, and a third time in Paris in September Press Release . In addition to OECD Member government officials, private sector representatives and experts on privacy, data protection and consumer protection participate in these meetings.
[http://www.oecd.org/dsti/iccp/legal/top-page.html]

World Intellectual Property Organization (WIPO)

WIPO is an intergovernmental organization with headquarters in Geneva, Switzerland. It is one of the 16 specialized agencies of the United Nations system of organizations, and is responsible for the promotion of the protection of intellectual property throughout the world , and for the administration of various multilateral treaties dealing with the legal and administrative aspects of intellectual property. Intellectual property comprises industrial property, chiefly in inventions, trademarks, industrial designs, and appellations of origin; and copyright, chiefly in literary, musical, artistic, photographic and audiovisual works. A substantial part of the activities and the resources of WIPO is devoted to development cooperation with developing countries.
[]

Global Electronic Commerce

The Administration developed A Framework for International Electronic Commerce that suggested a set of principles and a road map for international discussions and agreements to facilitate the growth of commerce on the Internet. The Framework recognized that the Global Information Infrastructure has the potential to revolutionize commerce and to accelerate the growth of trade. Principles expressed in the Framework include: the private sector should lead the expansion of the Internet; Governments should avoid undue restrictions on electronic commerce and recognize the unique qualities of cyberspace; and the Internet should be a truly international medium.
[http://nvl.nist.gov/]

G7

The G7 members along with the European Commission are supporting a group of projects involving international co-operation. These projects are directed toward demonstrating the potential of the Information Society and stimulate its deployment. The projects support the goal of international consensus on access to networks and applications and their interoperability; opportunities for information exchange; clearly understandable social, economic and cultural benefits which will demonstrate to the public the potential of the information society; identification of obstacles to a global information society; and creation of markets for new products and services. The U.S. government is contributing to the Global Inventory Project (GIP) which is creating an electronically accessible multimedia inventory of information regarding major national and international projects, studies and other data relevant to the promotion and the further development of knowledge of and understanding of the Information Society. The project builds upon and complements on-going national and international initiatives.

Government-Industry Cooperative Activities

Advisory Boards and Other Avenues for Solicitation of Industry Views

The U.S. Government makes extensive use of advisory boards and other groups to obtain the views and expertise of individuals and organizations outside the government. There are several such groups whose purpose is to assist the government in addressing IT security issues. Several of such groups are described below. (In addition to the URL references, if a given committee or group is sponsored or supported by a specific U.S. Government agency, that agency is indicated.)

Computer System Security and Privacy Advisory Board

Under the Computer Security Act of 1987, the U.S. Congress established the Computer System Security and Privacy Advisory Board (CSSPAB) as a public advisory board to NIST and the government in general on issues involving IT security. The board comprises twelve members, in addition to the Chairperson, who are recognized experts in the fields of computer and telecommunications systems security and technology. [http://csrc.ncsl.nist.gov/csspab] (See also National Institute of Standards and Technology (NIST))

Technical Advisory Committee To Develop A Federal Information Processing Standard for the Federal Key Management Infrastructure (TACDFIPFKMI)

The Technical Advisory Committee to develop a Federal Information Processing Standard for the Federal Key Management Infrastructure was established in late 1996. The objective of the committee is to make technical recommendations regarding the development of a draft Federal Information Processing Standard (FIPS) for the Federal Key Management Infrastructure. This committee began its work in early 1997. (See also *Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure*)

Commission on Critical Infrastructure Protection

The President and Congress believe certain national infrastructures are so vital that their incapacity or destruction would have a dramatic effect on the defense, economic security, and public welfare of the United States. Because many of the critical infrastructures are owned and operated privately, the administration realized the need for a partnership between the private sector and Government to address the issue. President Clinton established the Commission on Critical Infrastructure Protection by Executive Order 13010 on July 15, 1996.

The eight critical infrastructures include the electric power system, gas and oil (storage and transportation), telecommunications, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue) and continuity of government services . Threats to these infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").

The Commission is chaired by an individual from outside the Federal Government. Ten executive branch departments and agencies have each nominated a senior-level Federal employee and one other person from outside the Federal Government, bringing the total to twenty full-time commissioners. [www.pccip.gov]

National Security Telecommunications Advisory Committee

The NSTAC is a Presidential Advisory Committee that was established in September of 1982 to provide advice and expertise to the President and the Executive Agent, NCS, on issues and problems related to implementing NS/EP telecommunications policy.

The NSTAC consists of up to 30 senior corporate leaders representing major telecommunications-related industries, who provides a unique source of expertise not available elsewhere in the government. There are currently 27 NSTAC representatives. The NSTAC constitutes an opportunity for Federal departments and agencies to tap into a vast amount of telecommunications expertise.

The NSTAC's Industry Executive Subcommittee (IES), and the IES working groups, task forces, and other subordinate groups analyze NS/EP telecommunication issues and report their findings to the NSTAC to advise the President.

Because the NCS serves as the focal point for joint industry/government planning, the NSTAC and NCS have developed a close partnership. Through this partnership, the National Coordinating Center for Telecommunications (NCC) was established in 1984. The NCC is a joint government and industry operation for coordinating NS/EP telecommunication activities. [164.117.147.223/~ncs/html/nstac.htm]

National Research Council

The National Research Council was organized by the National Academy of Sciences to associate the broad community of science and technology with the Academy's purposes and general policies. The NRC's Computer Science and Technology Board conducts studies to evaluate trends in the development and diffusions of computer technology and their impacts. Issues in computer security, export controls, and threats have been subject of past reports issued by the NRC.

Independent Industry Special Interest Groups

In addition to specific industry groups established by the government for advice and expertise, there are several industry-sponsored groups that provide valuable input and opinion to the government.

Computer Systems Policy Project (CSPP)

CSPP CEOs develop and advocate public policy positions on trade and technology issues. Viewing both as interrelated, CSPP has offered thoughtful public policy proposals on market access, antidumping, and export control policy. CSPP has also made recommendations to the government on critical technology initiatives such as the National Information Infrastructure, federal R&D support, and federal laboratory research. CSPP continues to work on these and other issues that will help their industry, and others, meet the challenges of a leadership role in a global marketplace.

Computer Systems Policy Project (CSPP) member companies include: Apple, Compaq, Data General, Digital Equipment, Hewlett-Packard, IBM, NCR, Silicon Graphics, Stratus Computer, Sun Microsystems, Tandem , and Unisys.

[http://www.cspp.org:80/]

Cross Industry Working Team (XIWT)

XIWT aims to foster the understanding, development and application of technologies that cross industry boundaries, facilitate the conversion of the NII vision into real-world implementations, and facilitate a dialogue among representatives of stakeholders in the private and public sectors. XIWT will develop common technological and architectural approaches that bridge industry gaps and match the evolution of information technologies while providing for openness, heterogeneity, interoperability, scalability and ease of useplan information infrastructure pilot projects that leverage industry capabilities and state-of-the-art researchfoster ongoing experimentation and development of technology and cross-industry

applications and skillspromote cross-fertilization of technology and stimulate advanced infrastructure developmentcreate and sustain an open, cooperative networked environment for the members to exchange technical ideas, interests, and informationmaintain an open forum for dialogue among representatives of key U.S. stakeholders in the private and public sectorsorganize NII technology forums to discuss and disseminate XIWT results and sponsor periodic publications of White Papers on specific technology issuesbuild a common knowledge base for members on relevant topics.
XIWT Members participate actively in working teams, Plenary meetings, seminars and by other means to identify issues and solutions and work towards consensus on recommendations.
[http://www.cnri.reston.va.us:3000/XIWT/AboutXIWT/goals.html]

Standards Activities

American National Standards Institute Accredited Committee X9

Accredited by the American National Standards Institute (ANSI), X9 develops and publishes voluntary, consensus technical standards for the financial services industry. X9's inter-industry voting membership includes over 300 organizations representing investment managers, banks, software and equipment manufacturers, printers, credit unions, depositories, government regulators, associations, consultants, and others X9 develops Standards for check processing, electronic check exchange, PIN management and security, financial industry use of data encryption, and wholesale funds transfer, among others. American National Standards Institute Accredited Committee X3.T5 - U.S. Technical Advisory Group to International Standards Organization on common criteria.
[http://www.x9.org/x9/]

Accredited Standards Committee X3, Information Technology

X3 recently changed its name to the National Committee for Information Technology Standards. Its goal is to produce market-driven voluntary consensus standards in the areas of multimedia (MPEG/JPEG), intercommunication among computing devices and information systems (including the Information Infrastructure, SCSI-2 interfaces, Geographic Information Systems), storage media (hard drives, removable cartridges), database (including SQL3), security, and programming languages (such as C++). Technical Committee X3.T5 is the U.S. Technical Advisory Group to International Standards Organization on the common criteria project.

Institute of Electrical and Electronics Engineers

The IEEE carries out the development of voluntary industry standards in the fields of electrical engineering, electronics, radio, and the allied branches of engineering or related arts and sciences.

Open Group

The Open Group is an international consortium of vendors, ISVs and end-user customers from industry, government, and academia, dedicated to the advancement of multi-vendor information systems. The Open Group’s goal is to enable customer choice in the implementation of multi-vendor information systems. The Open Group concentrates on three main areas: the development and certification of platforms that further extend the portability and scalability of open systems; the establishment of secure, open and robust systems for electronic commerce, and open network computing. Initiatives are addressing security, interoperability, distributed systems management, architecture, and the Internet..

Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is the protocol engineering and development arm of the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Conclusions

It should be clear from this discussion, that the need for protection of the evolving global information infrastructure is well appreciated by both the U.S. Government and the private sector. If there is a problem, it is one of finding effective, non-monolithic ways to coordinate and communicate among the many "players" -- even within the U.S. Government itself. Thus, despite the increased level of activity, the basic inadequacy of security safeguards in the Internet (and in other aspects of information technology) continues. Most would agree, however, that clear progress is being made and that key security technologies are available and soon will be deployed widely.

Although this paper has focused primarily on areas in which the U.S. Government is involved, it must be recognized that the U.S. has limits to its influence in this area. From an international perspective, perhaps what is needed most are:

- Uniform international agreements on key issues such as privacy, data content, protection of intellectual property, and
- Information security fora that are truly international in scope.

Although the history of technological change has always been somewhat chaotic, the change itself has seldom, if ever, been so rapid and far-reaching. Thus, the importance of foresight and government-industry cooperation is crucial. Otherwise, the tremendous opportunities offered by information technology in general and such things as the Internet may actually lead to increase use of isolated networks and to specialized, unique, and non-interoperable solutions and applications -- or we will forego security altogether.

References

URLs

The following is a list of Uniform Reference Locators (URLs) to locations on the Internet/World Wide Web (WWW) that provide information on many of the entities and activities discussed in this paper.

Congress	http://thomas.loc.gov
National Security Council	http://www.whitehouse.gov/WH/EOP/NSC/html/nschome-plain.html
National Economic Council	http://www.whitehouse.gov/WH/EOP/nec/html/main.html
Office of Management and Budget	http://www2.whitehouse.gov/WH/EOP/OMB/html/ombhome.html
NIST	http://www.nist.gov
Bureau of Export Administration	http://www.bxa.doc.gov/
U.S. Patent and Trademark Office	http://www.uspto.gov/
National Security Agency	http://www.nsa.gov:8080/
DARPA	http://www.arpa.mil/index.html
Department of Treasury	http://www.ustreas.gov/
G7	http://www.ispo.cec.be/g7/summup.html
Department of Defense	http://www.disa.mil/
Open Group	http://www.opengroup.org/
Internet Engineering Task Force	http://www.ietf.cnri.reston.va.us/home.html
X3	http://www2.x3.org/ncits/
X9	http://www.x9.org/x9/